PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-012123
(43)Date of publication of application : 16.01.2001

(51)Int.CI. E05B 49/00
B60R 25/04
F02D 29/02
F02D 45/00
F02N 15/00

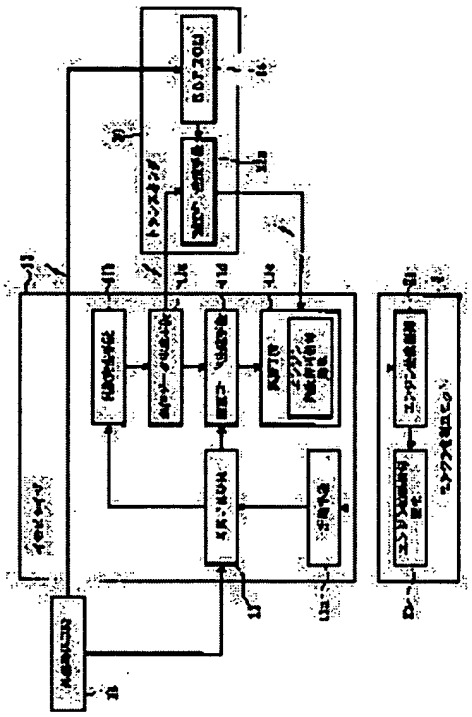
(21)Application number : 11-183808
(22)Date of filing : 29.06.1999

(71)Applicant : ASAHI DENSO CO LTD
(72)Inventor : SUZUKI MICHIYUKI

from CSP. III-A

(54) IMMOBILIZER, AND ATTESTING METHOD BY IMMOBILIZER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an immobilizer which is high in reliability of attestation, surely antitheft for a vehicle with its engine stopped, preventive from any misoperation, easy in fitting, and particularly effective for motorcycles, and an attestation method by the immobilizer.
SOLUTION: The random number data is generated based on the engine starting time data stored in a storage means, the random number data is transmitted to a transponder 20 through a radio part, the key specific information is coded using a specified coding method based on the random number data to generate the attestation code, the transponder 20 receives a generated attestation key in which the key specific information is coded using the coding method based on the random number data, an engine start permission signal is transmitted to an engine control unit 2 when the attestation code matches with the attestation key, and the time until the engine is started after a power source for an immobilizer 10 is turned on is stored in the storage means.



LEGAL STATUS

[Date of request for examination] 13.11.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－12123
（P2001－12123A）
(43)公開日　平成13年1月16日(2001.1.16)

(51)Int.Cl.'	識別記号	FI		テーマコード(参考)
E05B 49/00		E05B 49/00	K	2E250
B60R 25/04	610	B60R 25/04	610	3G084
F02D 29/02		F02D 29/02	K	3G093
45/00	345	45/00	345L	
F02N 15/00		F02N 15/00	F	

審査請求　未請求　請求項の数6　OL　（全 14 頁）

(21)出願番号　特願平11－183908

(22)出願日　平成11年6月29日(1999.6.29)

(71)出願人　000213954
朝日電装株式会社
静岡県浜北市中条1126番地

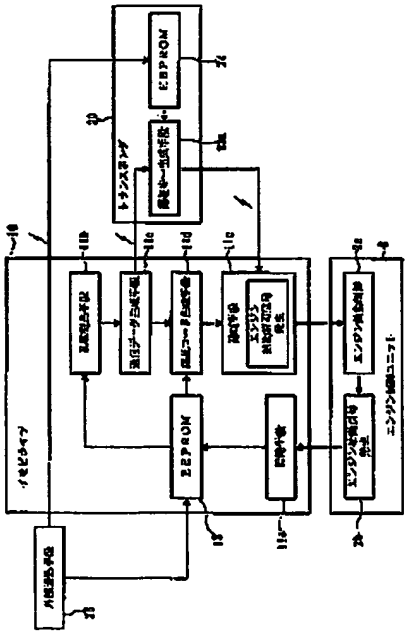
(72)発明者　鈴木　通之
静岡県浜北市中条1126番地　朝日電装株式会社内

(74)代理人　100095814
弁理士　越川　隆夫

最終頁に続く

(54)【発明の名称】　イモビライザ及びイモビライザによる認証方法

(57)【要約】
【課題】認証の信頼性が高く、エンジン停止中の車両に対して確実な盗難防止が可能で、誤動作を防止できると共に装着が容易で、特に二輪車に有効なイモビライザ及びイモビライザによる認証方法を提供することにある。
【解決手段】記憶手段に記憶されているエンジンの始動時間データを基に乱数データを生成し、無線部を介して乱数データをトランスポンダに送信すると共に、乱数データを基に所定の暗号化手法を用いてキーの固有情報を暗号化して認証コードを生成し、乱数データを基に該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化した生成した認証キーを受信し、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イモビライザの電源オンから、エンジンが始動するまでの時間を始動時間データとして記憶手段に記憶することを特徴とする。



1

【特許請求の範囲】

【請求項１】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザによる認証方法において、記憶手段にあらかじめ記憶されているエンジンの始動時間データを基に乱数データを生成し、次に、無線部を介して該乱数データを該トランスポンダに送信すると共に、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成し、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信した後、該認証コードと該認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、該イモビライザの電源オンから、該エンジンが始動するまでの時間を該始動時間データとして該記憶手段に記憶してなるイモビライザによる認証方法。

【請求項２】前記エンジンが始動した後、前記無線部を停止すると共に、前記イモビライザを休止してなる請求項１記載のイモビライザによる認証方法。

【請求項３】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザによる認証方法において、記憶手段にあらかじめ記憶されている該イモビライザの電源オン時間データを基に乱数データを生成し、次に、無線部を介して該乱数データを該トランスポンダに送信すると共に、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成し、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信した後、該認証コードと該認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イグニッションスイッチのオン／オフにより該イモビライザの電源のオン／オフを行い、該イモビライザの電源がオンされている時間を該電源オン時間データとして該記憶手段に記憶してなるイモビライザによる認証方法。

【請求項４】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザにおいて、該イモビライザの電源オンから、エンジンが始動するまでの時間をカウントして始動時間データを生成する計時手段と、該始動時間データを記憶する記憶手段と、該記憶手段に記憶されている始動時間データを基に乱数データを生成する乱数発生手段と、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、該トランスポンダに該乱数データを送信すると共に、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信する無線部と、該認証コードと該認証キーとが一致したときに、該エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、該始動時間データを用いて該キーを認証することを特徴とするイモビライザ。

2

【請求項５】前記エンジンが始動した後、前記無線部を停止すると共に、前記イモビライザを休止することを特徴とする請求項４記載のイモビライザ。

【請求項６】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザにおいて、イグニッションスイッチによりオン／オフする電源部と、該イモビライザの電源オン時間データを生成する計時手段と、該電源オン時間データを記憶する記憶手段と、該記憶手段に記憶されている電源オン時間データを基に乱数データを生成する乱数発生手段と、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、該トランスポンダに該乱数データを送信すると共に、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信する無線部と、該認証コードと該認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、該イモビライザの電源オン時間を用いて該キーを認証することを特徴とするイモビライザ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、自動二輪車や原動機付き自転車などの車両のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別し、車両の盗難を防止するためのイモビライザ及びイモビライザによる認証方法に関する。

【０００２】

【従来の技術】従来、車両の盗難を防止するためのイモビライザの一例として特開平１１－９１５０９号がある。同公報によれば、エンジン制御ユニットは、乱数を生成するシード生成手段と、乱数を外部へ送出するシード送信手段と、乱数を暗号化アルゴリズムにより暗号化して認証キーを生成する認証キー生成手段と、外部からキーを受信するキー受信手段と、外部からのキーと認証キーとを比較して、合致したときにセキュリティを解除する合致判定手段と、エンジンの回転数、燃料噴射量、吸入空気量、スロットル開度、水温、イグニッションスイッチのオン－オフ時のフリーランタイマの計時値などの車両制御情報を読み込む車両制御情報読込み手段とを備えている。

【０００３】また、ユーザー側キーユニットは、エンジン制御ユニットのシード送信手段からの乱数を受信するシード受信手段と、エンジン制御ユニットの認証キー生成手段と同一の暗号化アルゴリズムを有して、乱数を暗号化アルゴリズムにより暗号化してキーを生成するキー生成手段と、生成したキーをエンジン制御ユニットのキ

一受信手段へ送信するキー送信手段とを備えている。

【０００４】エンジン制御ユニットでは、車両制御情報読込み手段にてエンジンの回転数、燃料噴射量、吸入空気量、スロットル開度、水温などの車両制御情報を読込み、シード生成手段にて複数の車両制御情報の加算値として乱数を生成する。ユーザー側キーユニットでは、エンジン制御ユニットから乱数を受信し、キー生成手段にてシード生成手段と同一の暗号化アルゴリズムによりキーを生成し、このキーをエンジン制御ユニットへ送信する。そして、エンジン制御ユニットの合致判定手段にて、ユーザー側キーユニットからのキーを認証キーと比較して、合致したときにセキュリティを解除する。

【０００５】

【発明が解決しようとする課題】しかしながら、前記イモビライザにおいて、乱数を生成する基となる車両制御情報は、エンジンが動作している場合にのみ得られる情報であって、エンジン始動前に得られる情報ではない。このため、エンジンが動作していない車両に対するセキュリティ効果は有していない。

【０００６】また、同公報には、エンジン停止後のセキュリティを確保するために、イグニッションスイッチのオン－オフ時のフリーランタイマの計時値を使用することが書かれている。しかしながら、計時値をどのように保持し使用するのかについての記載がない。

【０００７】また、このイモビライザは、自動車のように、エンジンの回転数、燃料噴射量、吸入空気量、スロットル開度、水温などの高度な車両制御情報を収集している車両には適しているものの、原動機付き自転車のように、高度な車両制御情報を収集する必要のない車両においては、実用的ではない。

【０００８】また、既に市販され使用されている車両に、このイモビライザのみを装着することは困難であり、エンジン制御ユニットを交換することとなり、多額の費用がかかってしまう。

【０００９】本発明は、このような事情に鑑みてなされたもので、認証の信頼性が高く、エンジン停止中の車両に対して確実な盗難防止が可能で、誤動作を防止できると共に装着が容易で、特にエンジン制御ユニットが簡易な自動二輪車や原動機付き自転車などの二輪車に有効なイモビライザ及びイモビライザによる認証方法を提供することにある。

【００１０】

【課題を解決するための手段】請求項１記載のイモビライザによる認証方法は、記憶手段にあらかじめ記憶されているエンジンの始動時間データを基に乱数データを生成し、次に、無線部を介して乱数データをトランスポンダに送信すると共に、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成し、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化することにより生成した認証キーを受信した後、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イモビライザの電源オンから、エンジンが始動するまでの時間を始動時間データとして記憶手段に記憶することを特徴とする。

【００１１】請求項２記載のイモビライザによる認証方法は、エンジンが始動した後、無線部を停止すると共に、イモビライザを休止することを特徴とする。

【００１２】請求項３記載のイモビライザによる認証方法は、記憶手段にあらかじめ記憶されているイモビライザの電源オン時間データを基に乱数データを生成し、次に、無線部を介して乱数データをトランスポンダに送信すると共に、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成し、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化することにより生成した認証キーを受信した後、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イグニッションスイッチのオン／オフによりイモビライザの電源のオン／オフを行い、イモビライザの電源がオンされている時間を電源オン時間データとして記憶手段に記憶することを特徴とする。

【００１３】請求項４記載のイモビライザは、イモビライザの電源オンから、エンジンが始動するまでの時間をカウントして始動時間データを生成する計時手段と、始動時間データを記憶する記憶手段と、記憶手段に記憶されている始動時間データを基に乱数データを生成する乱数発生手段と、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、トランスポンダに乱数データを送信すると共に、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化することにより生成した認証キーを受信する無線部と、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、始動時間データを用いてキーを認証することを特徴とする。

【００１４】請求項５記載のイモビライザは、エンジンが始動した後、無線部を停止すると共に、イモビライザを休止することを特徴とする。

【００１５】請求項６記載のイモビライザは、イグニッションスイッチによりオン／オフする電源部と、イモビライザの電源オン時間データを生成する計時手段と、電源オン時間データを記憶する記憶手段と、記憶手段に記憶されている電源オン時間データを基に乱数データを生成する乱数発生手段と、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、トランスポンダに乱数データを送信すると共に、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有

情報を暗号化することにより生成した認証キーを受信する無線部と、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、イモビライザの電源オン時間を用いてキーを認証することを特徴とする。

【００１６】

【発明の実施の形態】以下、本発明の形態について図面を参照しながら具体的に説明する。図１、図３及び図４は第１の実施例を示す図面、図５～図７は第２の実施例を示す図面である。尚、図２は、第１の実施例と第２の実施例に共通する図面である。

【００１７】（実施の形態１）図１は本発明のイモビライザの第１の実施例を示す構成図、図２は本発明のトランスポンダの一実施例を示す構成図である。図３は図１のイモビライザの動作の様子を示す構成図である。図４は図１のイモビライザの動作を示すフローチャートである。

【００１８】図１～図４において、イモビライザ１０は、自動二輪車や原動機付き自転車などの車両のキー３に内蔵されたトランスポンダ２０との間で無線通信を行い、トランスポンダ２０から送られる情報を基に、キー３がその車両固有のものであるかどうか識別し、車両の盗難を防止するための装置である。イモビライザ１０は、ＣＰＵ（central processing unit）１１、電源部１２、ＥＥＰＲＯＭ（Electrically Erasable and Programmable Read Only Memory）１３、通信インターフェース１４、無線部１５により構成されている。

【００１９】ＣＰＵ１１は中央演算装置であって、イモビライザ１０の動作を制御するものである。電源部１２は、イモビライザ１０が動作するための直流電源であるＶＤＤ１７を、バッテリー７から作り出すためのものである。尚、バッテリー７は、キーシリンダ４内に設けられたイグニッションスイッチ５を介して電源部１２に接続されている。このイグニッションスイッチ５は、キー３をキーシリンダ４に挿入して運転位置に回転セットしたときにオンとなるスイッチである。ＥＥＰＲＯＭ１３は、ＣＰＵ１１に接続された記憶手段であり、不揮発性である。尚、この実施の形態１については、ＥＥＰＲＯＭ１３を記憶手段として使用しているが不揮発性の記憶手段であればこれに限られるものではなく、例えば、ＥＰＲＯＭ（Erasable and Programmable Read Only Memory）、ＯＴＰ（One Time Programmable read only memory）、フラッシュＥＥＰＲＯＭ、その他電源バックアップ機能付きのメモリ等が使用可能である。

【００２０】通信インターフェース１４は、ＣＰＵ１１とエンジン制御ユニット２とが通信するための仲介役であり、両者間の信号レベルや信号形式を整合させるものである。本実施の形態１においては、車両のエンジンの始動や停止を制御するためエンジン制御ユニット２と通信インターフェース１４との間の通信は、シリアル信号

（例えばＲＳ－２３２Ｃ準拠の信号）を使用している。これは、エンジン制御ユニット２に送る情報を複雑にし、外部から解読しにくくするためである。しかしながら、これに限られるものではなく、レベルの高低だけのＩ／Ｏ信号であっても差し支えない。尚、ＣＰＵ１１と通信インターフェース１４とはバスにより接続されている。

【００２１】無線部１５は、ＣＰＵ１１から送られてくる情報を変調するものであり、変調された無線信号は、キーシリンダ４に内蔵されたアンテナ６からトランスポンダ２０のアンテナ２５に送られる。また、無線部１５は、トランスポンダ２０から送信された無線信号を、アンテナ６で受信して復調し、復調した情報をＣＰＵ１１に送る。無線部１５とＶＤＤ１７との間には、無線部電源スイッチ１６が設けられており、ＣＰＵ１１の指令により、無線部１５の電源はオン／オフ可能となっている。

【００２２】トランスポンダ２０は、イモビライザ１０から送られる無線信号を基に動作し、その無線信号に対しての回答となる信号を無線信号としてイモビライザ１０に送信するものである。トランスポンダ２０は、キー３に内蔵されている。トランスポンダ２０は、イモビライザ１０から送られる無線信号を受信したり、トランスポンダ２０側で生成した情報を送信するためのアンテナ２５、無線信号を変復調するための無線部２２、トランスポンダ２０の制御を行う認証キー生成ＩＣ２３、キー固有の情報を格納する不揮発性の記憶手段であるＥＥＰＲＯＭ２４と２次電池に相当するコンデンサ２１から構成される。

【００２３】次に、イモビライザ１０の動作を説明する。尚、以下の説明において、括弧内の符号は図４のフローチャートの符号に対応している。運転者がキー３を用いて車両を始動させようとする場合は、まず、運転者はキー３をキーシリンダ４に挿入する。そして、キー３を運転位置（オン位置）に回す。すると、イグニッションスイッチ５がオンして、電源部１２にバッテリ７が接続される。そして、ＶＤＤ１７が電源部１２から出力され、イモビライザ１０が動作を開始する。

【００２４】イモビライザ１０が動作を開始すると、まず最初に、ＣＰＵ１１はソフトウェアで実現されている計時手段１１ａによりイモビライザ１０が動作している時間の計時を開始する（Ｓ１００）。つぎに、エンジンが動作しているかを、エンジン制御ユニット２からエンジン始動信号線２ｓを介して送られるエンジン始動信号により確認する（Ｓ１０１）。キー３挿入当初はエンジンは始動していないので、ＣＰＵ１１はＥＥＰＲＯＭ１３に格納されている始動時間データを読み出す（Ｓ１０２）。尚、始動時間データは、イモビライザ１０の動作開始からエンジン始動までの時間を計時手段１１ａで計時して生成したデータであり、前回エンジンを始動させ

て時の始動時間データが、あらかじめＥＥＰＲＯＭ１３に記憶されている。始動時間データの生成のタイミング等は後述する。また、車両を生産して初めてエンジンを始動させる時点でＥＥＰＲＯＭ１３に記憶されているデータは、時間０のデータである。

【００２５】次に、ＣＰＵ１１は乱数発生手段１１ｂにより、読み出した始動時間データを基に、乱数データを発生させる（Ｓ１０３）。発生させる乱数データの大きさは、例えば１０桁である。そして、ＣＰＵ１１は送信データ生成手段１１ｃにより、無線部１５からトランスポンダ２０に送信するための送信データを生成する（Ｓ１０４）。この送信データ生成手段１１ｃを介することなく、乱数データを直接無線部１５から送信させることは可能である。しかしながら、本実施の形態１においては、乱数データに車種を限定するための情報を付加して、送信データを生成している。すなわち、例えば車種を限定するための２桁のパスワードを乱数データの先頭に付け加えている。パスワードの機能・効果については後述する。そして、生成された送信データを無線部１５からトランスポンダ２０に送信する（Ｓ１０５）。

【００２６】トランスポンダ２０側では、イモビライザ１０からの送信データをアンテナ２５を介して無線部２２で受信する（Ｓ１５１）。無線部２２で復調されたパスワード＋乱数データを基に、認証キー生成ＩＣ２３内の認証キー生成手段２３ａにより、認証キーを生成する（Ｓ１５２）。認証キーは、ＥＥＰＲＯＭ２４に記憶されているキー３固有の情報である暗号キーを用いて、乱数データを暗号化したもので、例えば、２４ビットのデータである。尚、暗号化の方法は特に限定されるものではなく、例えばＤＥＳ（Data Encryption Standard；１９７７年米国商務省標準局が制定）等の方式が使用可能である。トランスポンダ２０は、生成した認証キーを無線部２２及びアンテナ２５を介してイモビライザ１０に送信する（Ｓ１５３）。

【００２７】トランスポンダ２０の認証キー生成手段２３ａは、イモビライザ１０の情報を受信するとすぐに動作するのではなく、まず、パスワードの内容が、認証キーの生成を行ってもよいものであるかを確認する。当然、不正なパスワードであったり、パスワードがはじめから含まれていない場合には、トランスポンダ２０は認証キーの生成及び送信を行わない。このように、トランスポンダ２０側からの認証キーの発信を制限することで、このキー３が他車種のイモビライザに接近した場合に、不必要な信号を発信しないようにすることができ、複数のキーを１つのキーホルダに束ねている場合などに、他車両の正規な認証に混信を与えるのを防止可能である。

【００２８】トランスポンダ２０は電池を有しておらず、イモビライザ１０の無線部１５から、パスワード＋乱数データの前に送られる電力信号により、無線部２２を動作させると共に、コンデンサ２１を帯電する。すなわち、コンデンサ２１は、イモビライザ１０の無線部１５から送られる電力信号により、２次電池として充電され、トランスポンダ２０を動作させる。

【００２９】トランスポンダ２０が認証キーを生成している間に、イモビライザ１０側では認証コードの生成を、ＣＰＵ１１の認証コード生成手段１１ｄにおいて行う（Ｓ１０６）。認証コードは、パスワード＋乱数データを基に、ＥＥＰＲＯＭ１３に記憶されているキー３固有の情報である暗号キーを用いて、乱数データを暗号化したものである。尚、暗号化の方式は、トランスポンダ２０で使用されているものと同一のものである。

【００３０】次に、イモビライザ１０は、トランスポンダ２０からの認証キーを受信する（Ｓ１０７）。そして、ＣＰＵ１１の認証手段１１ｅにおいて、認証コードと認証キーの比較認証を行う（Ｓ１０８）。認証コードと認証キーとが一致した場合には、エンジン始動許可信号を発生する。このエンジン始動許可信号はＣＰＵ１１から、通信インターフェース１４を介して、エンジン制御ユニット２に送られる（Ｓ１０９）。エンジン始動許可信号を受信したエンジン制御ユニット２は、エンジン始動制御２ａを行いエンジンを始動させる。実際の自動車や自動二輪車等においては、エンジン始動許可信号によりエンジン始動可能状態となり、運転者のスタースイッチ（スタートスイッチ）のオンにより、エンジンの始動が行われる。エンジン制御ユニット２は、エンジンの始動を確認すると、イモビライザ１０に対して、エンジン始動信号完生２ｂを行う。

【００３１】イモビライザ１０は、あらためてエンジン始動を確認する（Ｓ１０１）。ここで、エンジンの始動を確認すると、計時手段１１ａによる始動信号の計時を終了し、計時した始動時間データをＥＥＰＲＯＭ１３に書込み、前回始動時のデータを更新する（Ｓ１１１）。更新の方法としては、ＥＥＰＲＯＭ１３にすでに書き込まれている始動時間データに新たな始動時間データを足し合わせて新たな始動時間データを生成してもよいし、新たな始動時間データを前回の始動時間データと置き換えてしまってもよい。

【００３２】次に、ＣＰＵ１１は無線部電源スイッチ１６をオフして、無線部１５を停止させる（Ｓ１１２）。そして、一連のキー認証作業を終えた後に、ＣＰＵ１１を休止状態にすることにより、イモビライザ１０を休止させる（Ｓ１１３）。

【００３３】尚、本実施の形態１においては、始動時間の計時の開始をイモビライザ１０の動作開始時としているが、計時開始をイモビライザ１０がエンジン始動許可信号を出力した時としてもよい。

【００３４】また、本実施の形態１において、計時手段１１ａ、乱数発生手段１１ｂ、送信データ生成手段１１ｃ、認証コード生成手段１１ｄ及び認証手段１１ｅは、

ＣＰＵ１１によりソフトウェアとして実現されている。しかしながら、これらの手段を、ＣＰＵ１１を用いることなく、論理回路などのハードウェア回路のみで構成することも可能であるし、ソフトウェアとハードウェアとの混在により実現することも可能である。

【００３５】尚、ＥＥＰＲＯＭ１３にキー３に固有の暗号キーを書き込むには、エンジン制御ユニット２に換えて、パーソナルコンピュータなどの外部書込手段２８を接続し、通信インターフェース１４及びＣＰＵ１１を介して、ＥＥＰＲＯＭ１３の書込を行う。トランスポンダ２０のＥＥＰＲＯＭ２４の書込に関しては、イモビライザ１０のＥＥＰＲＯＮ１３を書き込むのと同じように外部書込手段２８をイモビライザ１０に接続し、イモビライザ１０からの無線信号でＥＥＰＲＯＭ２４の書込を行う。

【００３６】本実施の形態１においては、イモビライザ１０の電源オンからエンジンが始動するまでの時間である始動時間データを基に乱数データを生成し、その乱数データを基にキー３の固有情報を暗号化することにより認証キー及び認証コードを生成し、この認証キー及び認証コードを用いてキーの認証を行っている。イモビライザ１０の電源オンからエンジンが始動するまでの時間は、エンジンが始動する毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この始動時間データを基に生成された乱数データは、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。

【００３７】また、始動時間データをＥＥＰＲＯＭ１３に記憶しておき、次にエンジンを始動する時には、ＥＥＰＲＯＭ１３にあらかじめ記憶されている始動時間データを基に乱数データを生成している。このため、エンジン停止中の車両に対してより確実な盗難防止が可能である。

【００３８】また、エンジンが始動したかどうかの情報のみをエンジン制御ユニット２から受け取ることで始動時間データを生成することができるため、エンジン制御ユニット３が出力しなければならない情報は１つだけであり、高性能で高価なエンジン制御ユニット３を必要とせず、エンジン制御ユニット３の負担を軽減し、特にエンジン制御ユニット３が簡易な自動二輪車や原動機付き自転車などの二輪車に有効である。

【００３９】また、エンジンの始動により無線部１５を停止すると共に、イモビライザ１０を休止していることから、エンジン始動後のイモビライザ１０の誤動作を防止できると共に、エンジン停止などのエンジンの誤動作を防止できる。

【００４０】（実施の形態２）図５は本発明のイモビライザの第２の実施例を示す構成図である。図６は図５のイモビライザの動作の様子を示す構成図である。図７は図５のイモビライザの動作を示すフローチャートである。

【００４１】図５～図７において、イモビライザ３０は、自動二輪車や原動機付き自転車などの車両のキー３に内蔵されたトランスポンダ２０との間で無線通信を行い、トランスポンダ２０から送られる情報を基に、キー３がその車両固有のものであるかどうか識別し、車両の盗難を防止するための装置である。イモビライザ３０は、ＣＰＵ（central processing unit）３１、電源部１２、ＥＥＰＲＯＭ（Electrically Erasable and Programmable Read Only Memory）１３、通信インターフェース３４、無線部３５により構成されている。

【００４２】通信インターフェース３４は、ＣＰＵ３１とエンジン制御ユニット２８が通信するための仲介役であり、両者間の信号レベルや信号形式を整合させるものである。信号レベルや信号形式については、実施の形態１と同様である。

【００４３】無線部３５は、ＣＰＵ１１から送られてくる情報を変調するものであり、変調された無線信号は、キーシリンダ４に内蔵されたアンテナ６からトランスポンダ２０のアンテナ２５に送られる。また、無線部１５は、トランスポンダ２０から送信された無線信号を、アンテナ６で受信して復調し、復調した情報をＣＰＵ３１に送る。尚、ＥＥＰＲＯＭ１３、電源部１２及びトランスポンダ２０については、実施の形態１と同様なので説明を省略する。

【００４４】次に、イモビライザ３０の動作を説明する。尚、以下の説明において、括弧内の符号は図７のフローチャートの符号に対応している。運転者がキー３を用いて車両を始動させようとする場合は、まず、運転者はキー３をキーシリンダ４に挿入する。そして、キー３を運転位置（オン位置）に回す。すると、イグニッションスイッチ５がオンして、電源部１２にバッテリ７が接続される。そして、ＶＤＤ１７が電源部１２から出力され、イモビライザ３０が動作を開始する。

【００４５】イモビライザ３０が動作を開始すると、ＣＰＵ３１はＥＥＰＲＯＭ１３に格納されている電源オン時間データを読み出す（Ｓ２０２）。尚、電源オン時間データは、イモビライザ３０の動作開始からイモビライザ３０が電源オフまでの時間を計時手段３１ａで計時して生成したデータであり、前回イモビライザ３０を動作させた時の電源オン時間データが、あらかじめＥＥＰＲＯＭ１３に記憶されている。電源オン時間データの生成のタイミング等は後述する。また、車両を生産して初めてエンジンを始動させる時点でＥＥＰＲＯＭ１３に記憶されているデータは、時間０のデータである。

【００４６】次に、ＣＰＵ１１は乱数発生手段３１ｂにより、読み出した電源オン時間データを基に、乱数データを発生させる（Ｓ２０３）。発生させる乱数データの大きさは、例えば１０桁である。そして、ＣＰＵ３１は送信データ生成手段３１ｃにより、無線部３５からトラ

ンスポンダ２０に送信するための送信データを生成する（Ｓ２０４）。この送信データ生成手段３１ｃを介することなく、乱数データを直接無線部３５から送信させることは可能である。しかしながら、本実施の形態２においては、乱数データに車種を限定するための情報を付加して、送信データを生成している。すなわち、例えば車種を限定するための２桁のパスワードを乱数データの先頭に付け加えている。パスワードの機能・効果については後述する。そして、生成された送信データを無線部１５からトランスポンダ２０に送信する（Ｓ２０５）。

【００４７】トランスポンダ２０側では、イモビライザ３０からの送信データをアンテナ２５を介して無線部２２で受信する（Ｓ２５１）。無線部２２で復調されたパスワード＋乱数データを基に、認証キー生成ＩＣ２３内の認証キー生成手段２３ａにより、認証キーを生成する（Ｓ２５２）。認証キーは、ＥＥＰＲＯＭ２４に記憶されているキー３固有の情報である暗号キーを用いて、乱数データを暗号化したもので、例えば、２４ビットのデータである。尚、暗号化の方法は特に限定されるものではなく、例えばＤＥＳ（Data Encryption Standard；１９７７年米国商務省標準局が制定）等の方式が使用可能である。トランスポンダ２０は、生成した認証キーを無線部２２及びアンテナ２５を介してイモビライザ３０に送信する（Ｓ２５３）。

【００４８】トランスポンダ２０の認証キー生成手段２３ａは、イモビライザ３０の情報を受信するとすぐに動作するのではなく、まず、パスワードの内容が、認証キーの生成を行ってもよいものであるかを確認する。当然、不正なパスワードであったり、パスワードがはじめから含まれていない場合には、トランスポンダ２０は認証キーの生成及び送信を行わない。このように、トランスポンダ２０側からの認証キーの発信を制限することで、このキー３が他車種のイモビライザに接近した場合に、不必要な信号を発信しないようにすることができ、複数のキーを１つのキーホルダに束ねている場合などに、他車両の正規な認証に混信を与えるのを防止可能である。

【００４９】トランスポンダ２０は電池を有しておらず、イモビライザ３０の無線部３５から、パスワード＋乱数データの前に送られる電力信号により、無線部２２を動作させると共に、コンデンサ２１を蓄電する。すなわち、コンデンサ２１は、イモビライザ３０の無線部３５から送られる電力信号により、２次電池として充電され、トランスポンダ２０を動作させる。

【００５０】トランスポンダ２０が認証キーを生成している間に、イモビライザ３０側では認証コードの生成を、ＣＰＵ３１の認証コード生成手段３１ｄにおいて行う（Ｓ２０６）。認証コードは、パスワード＋乱数データを基に、ＥＥＰＲＯＭ１３に記憶されているキー３固有の情報である暗号キーを用いて、乱数データを暗号化したものである。尚、暗号化の方式は、トランスポンダ２０で使用されているものと同一のものである。

【００５１】次に、イモビライザ３０は、トランスポンダ２０からの認証キーを受信する（Ｓ２０７）。そして、ＣＰＵ３１の認証手段３１ｅにおいて、認証コードと認証キーの比較認証を行う（Ｓ２０８）。認証コードと認証キーとが一致した場合には、エンジン始動許可信号を発生する。このエンジン始動許可信号はＣＰＵ３１から、通信インターフェース３４を介して、エンジン制御ユニット２に送られる（Ｓ２０９）。エンジン始動許可信号を受信したエンジン制御ユニット２は、エンジン始動制御２ａを行いエンジンを始動させる。実際の自動車や自動二輪車等においては、エンジン始動許可信号によりエンジン始動可能状態となり、運転者のスタータースイッチ（スタートスイッチ）のオンにより、エンジンの始動が行われる。

【００５２】その後、イモビライザ３０は、１０分経過毎にＥＥＰＲＯＭ１３に納められている電源オン時間データを計時手段３１ａにより１加算してＥＥＰＲＯＭ１３に格納する（Ｓ２１１）。すなわち、イモビライザ３０が動作する毎に、動作している時間に見合った数値が足されることになる。尚、加算の間隔は１０分としたがこれに限られるものではなく、任意に定められるものである。イグニッションスイッチ５をオフすれば、イモビライザ３０の動作は停止し、同時に電源オン時間データの加算変更を停止される。尚、本実施の形態２では、前回イモビライザ３０を動作させて時の電源オン時間データに、現在の動作時間を引き続き加算しているがこれに限られるものではなく、認証終了後に一過電源オン時間データを消去してしまい新たに計時を始めてもよい。

【００５３】また、本実施の形態２おいて、計時手段３１ａ、乱数発生手段３１ｂ、送信データ生成手段３１ｃ、認証コード生成手段３１ｄ及び認証手段３１ｅは、ＣＰＵ３１によりソフトウェアとして実現されている。しかしながら、これらの手段を、ＣＰＵ３１を用いることなく、論理回路などのハードウェア回路のみで構成することも可能であるし、ソフトウェアとハードウェアとの混在により実現することも可能である。尚、ＥＥＰＲＯＭ１３にキー３に固有の暗号キーを書き込む方法は、実施の形態１と同様のため説明を省略する。

【００５４】本実施の形態２においては、イグニッションスイッチ５のオン／オフによりイモビライザ３０の電源のオン／オフを行い、イモビライザ３０の電源がオンされている時間を電源オン時間データとしており、この電源オン時間データを用いてキーを認証している。イモビライザ３０が電源オンしている時間は、車両の運転毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この電源オン時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。

【００５５】また、エンジン制御ユニット２から情報を得なくとも、キー３の認証が可能であることから、新たにエンジン制御ユニット２を設計し直す必要が無く、盗難防止装置としてのコストを抑えることができる。また、既に販売され、使用されている車両に対しても、エンジン制御ユニット２の機能に左右されることなく、容易にイモビライザ３０の装着ができる。

【００５６】

【発明の効果】請求項１の発明によれば、イモビライザの電源オンからエンジンが始動するまでの時間である始動時間データを基に乱数を生成し、その乱数を基にキーの固有情報を暗号化することにより認証キー及び認証コードを生成し、この認証キー及び認証コードを用いてキーの認証を行っている。イモビライザの電源オンからエンジンが始動するまでの時間は、エンジンが始動する毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この始動時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、始動時間データを記憶手段に記憶しておき、次にエンジンを始動する時には、記憶手段にあらかじめ記憶されている始動時間データを基に乱数を生成している。このため、エンジン停止中の車両に対してより確実な盗難防止が可能である。また、エンジンが始動したかどうかの情報のみをエンジン制御ユニットから受け取ることで始動時間データを生成することができるため、エンジン制御ユニットが出力しなければならない情報は１つだけであり、高性能で高価なエンジン制御ユニットを必要とせず、エンジン制御ユニットの負担を軽減し、特にエンジン制御ユニットが簡易な自動二輪車や原動機付き自転車などの二輪車に有効である。

【００５７】請求項２記載の発明によれば、エンジンの始動により無線部を停止すると共に、イモビライザを休止していることから、エンジン始動後のイモビライザの誤動作を防止できると共に、エンジン停止などのエンジンの誤動作を防止できる。

【００５８】請求項３の発明によれば、イグニッションスイッチのオン／オフによりイモビライザの電源のオン／オフを行い、イモビライザの電源がオンされている時間を電源オン時間データとしており、この電源オン時間データを用いてキーを認証している。イモビライザが電源オンしている時間は、車両の運転毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この電源オン時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、エンジン制御ユニットから情報を得なくとも、キーの認証が可能であることから、新たにエンジン制御ユニットを設計し直す必要が無く、盗難防止装置としてのコストを抑えることができる。また、既に販売され、使用されている車両

に対しても、エンジン制御ユニットの機能に左右されることなく、容易にイモビライザの装着ができる。

【００５９】請求項４の発明によれば、計時手段により、イモビライザの電源オンから、エンジンが始動するまでの時間をカウントした始動時間データが生成され、この始動時間データを基に乱数発生部が乱数を生成し、その乱数を基にキーの固有情報を暗号化することにより認証キー及び認証コードを生成し、認証手段が認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する。始動時間データは、エンジンが始動する毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この始動時間データを基に生成された乱数は推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、始動時間データを記憶手段に記憶しておき、次にエンジンを始動する時には、記憶手段に記憶されている始動時間データを基に乱数を生成している。このため、エンジン停止中の車両に対してより確実な盗難防止が可能である。また、エンジンが始動したかどうかの情報のみをエンジン制御ユニットから受け取ることで始動時間データを生成しているため、エンジン制御ユニットが出力しなければならない情報は１つだけであり、高性能で高価なエンジン制御ユニットを必要とせず、エンジン制御ユニットの負担を軽減し、特にエンジン制御ユニットが簡易な自動二輪車や原動機付き自転車などの二輪車に有効である。

【００６０】請求項５の発明によれば、エンジンの始動により無線部を停止すると共に、イモビライザを休止していることから、エンジン始動後のイモビライザの誤動作を防止できると共に、エンジン停止などのエンジンの誤動作を防止できる。

【００６１】請求項６の発明によれば、イグニッションスイッチによりオン／オフする電源部を備え、電源部がオンされている時間を電源オン時間データとしており、この電源オン時間データを用いてキーを認証している。イモビライザが電源オンしている時間は、車両の運転毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この電源オン時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、エンジン制御ユニットから情報を得なくとも、キーの認証が可能であることから、新たにエンジン制御ユニットを設計し直す必要が無く、盗難防止装置としてのコストを抑えることができる。また、既に販売され、使用されている車両に対しても、エンジン制御ユニットの機能に左右されることなく、容易にイモビライザの装着ができる。

【図面の簡単な説明】

【図１】本発明のイモビライザの第１の実施例を示す構成図である。

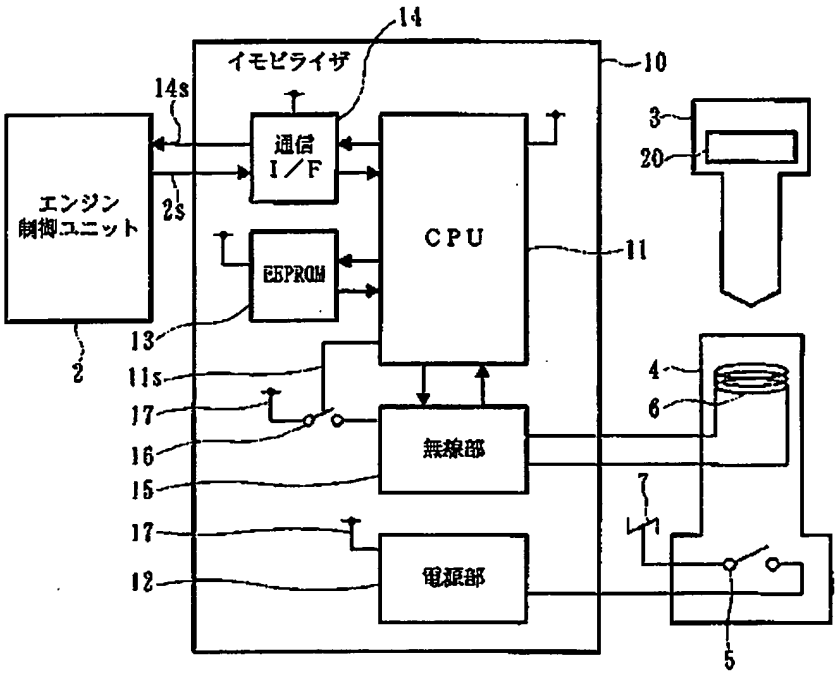
15

【図２】本発明のトランスポンダの一実施例を示す構成図である。
【図３】図１のイモビライザの動作の様子を示す構成図である。
【図４】図１のイモビライザの動作を示すフローチャートである。
【図５】本発明のイモビライザの第２の実施例を示す構成図である。
【図６】図５のイモビライザの動作の様子を示す構成図である。
【図７】図５のイモビライザの動作を示すフローチャートである。
【符号の説明】
２．８・・・・・・・・エンジン制御ユニット　＊

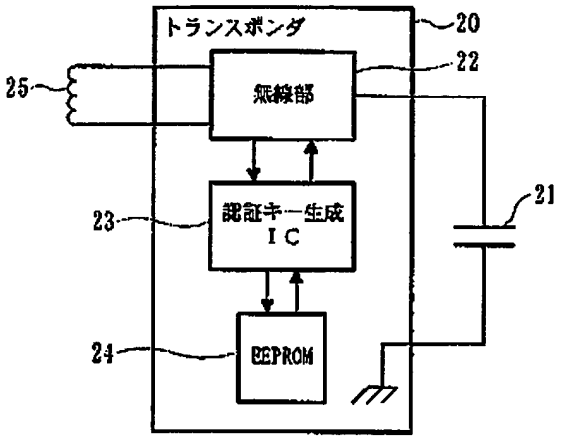
16

＊３・・・・・・・・・・キー
４・・・・・・・・・・キーシリンダ
５・・・・・・・・・・イグニッションスイッチ
６、２５・・・・・・・アンテナ
１０、３０・・・・・・イモビライザ
１１、３１・・・・・・ＣＰＵ
１２・・・・・・・・・電源部
１３、２４・・・・・・ＥＥＰＲＯＭ
１４、３４・・・・・・通信インターフェース
１５、２２・・・・・・無線部
１６・・・・・・・・・無線部電源スイッチ
２０・・・・・・・・・トランスポンダ
２３・・・・・・・・・認証キー生成ＩＣ

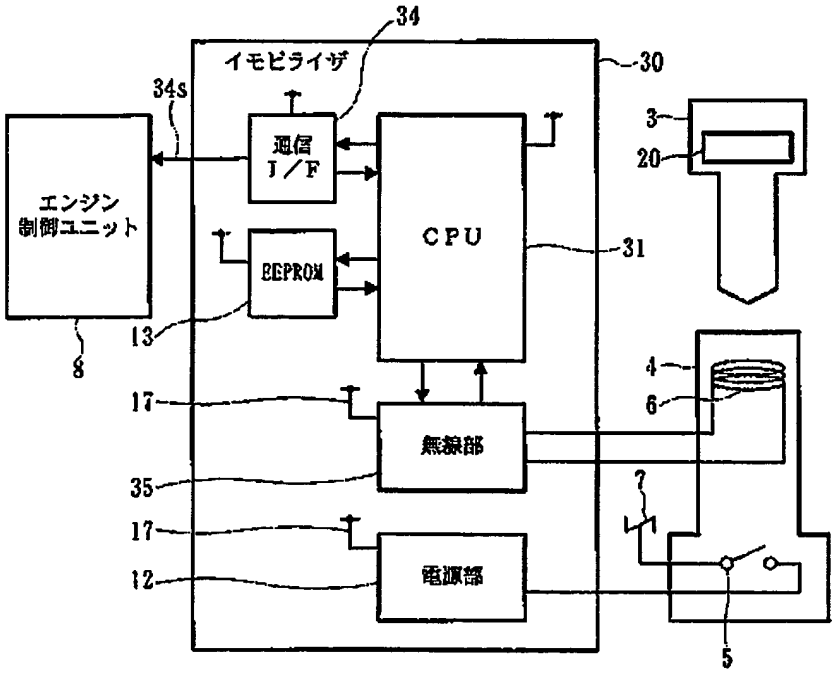
【図１】



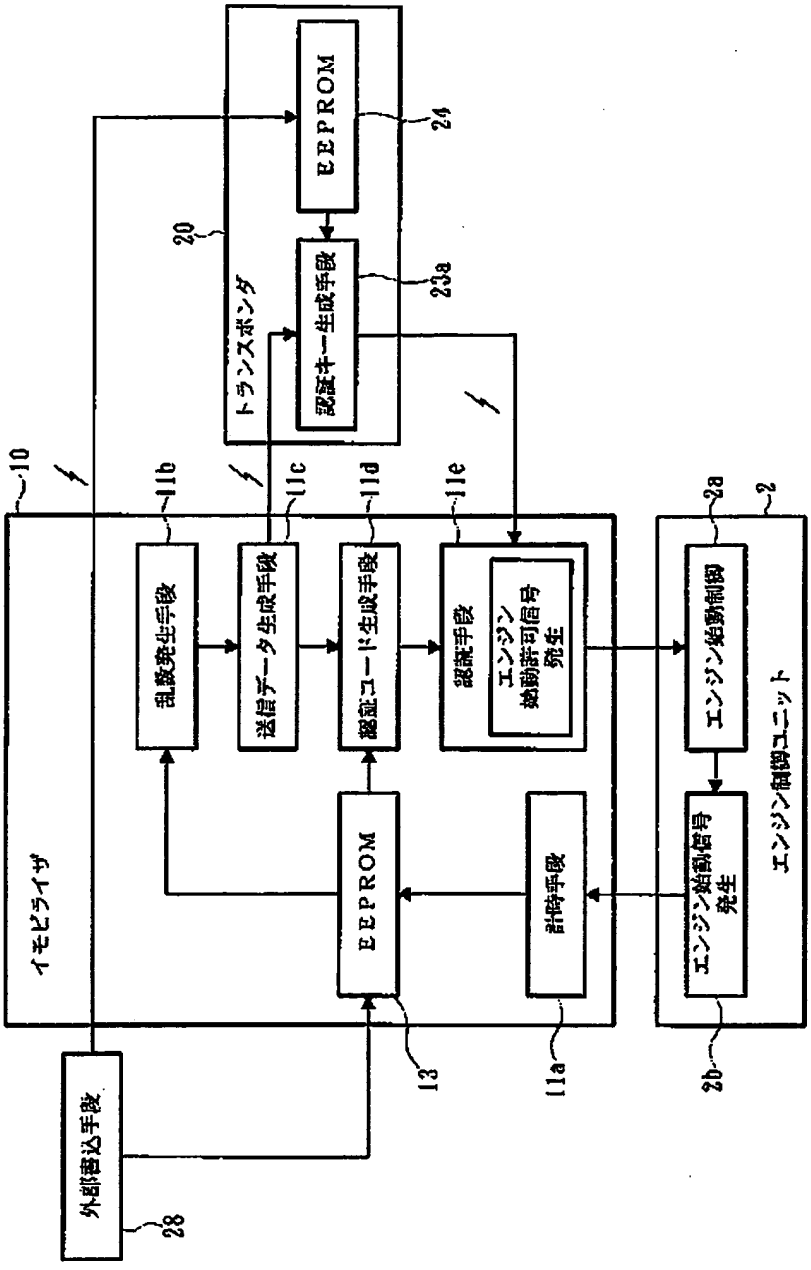
【図2】


トランスポンダ
20
22
25
無線部
23
認証キー生成
IC
21
24
EEPROM

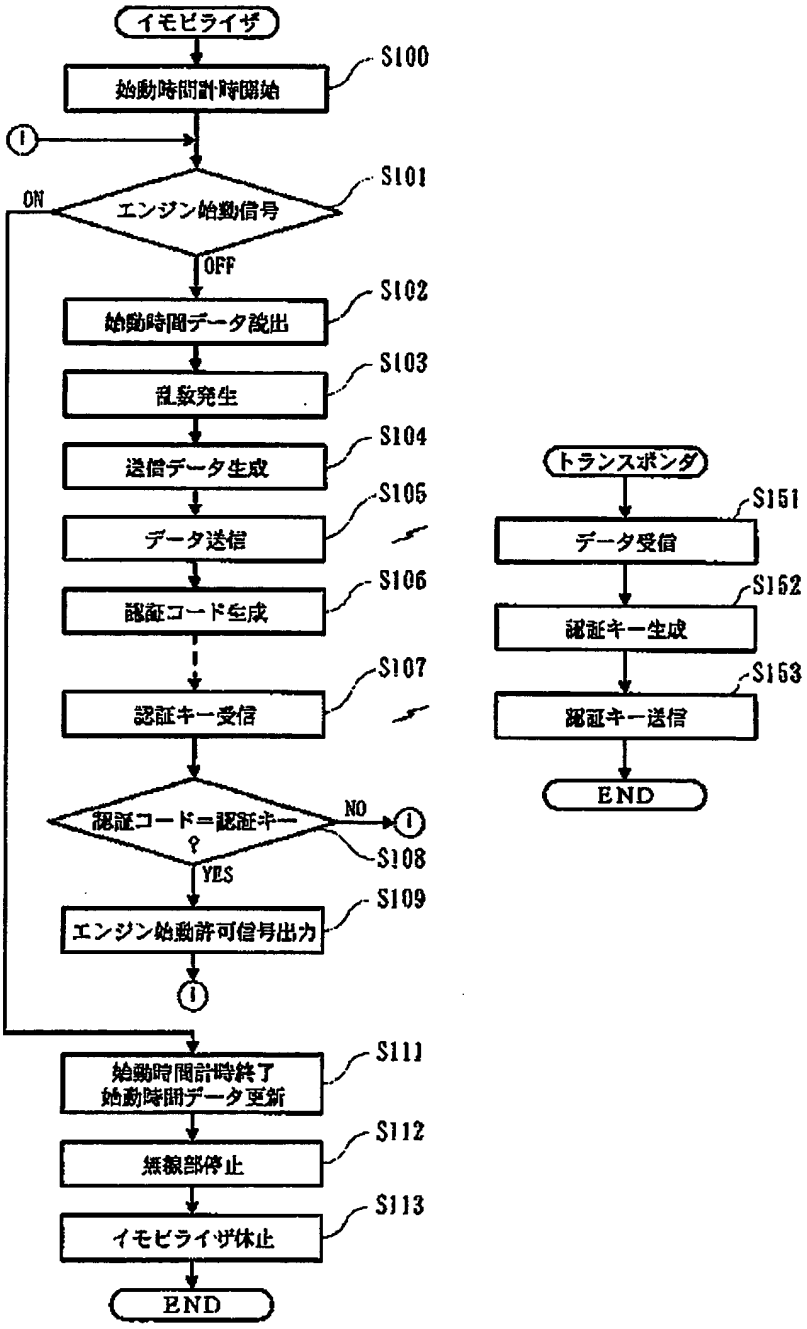
【図5】


34
イモビライザ
30
34s
通信
I/F
CPU
31
エンジン
制御ユニット
EEPROM
13
8
3
20
4
6
17
無線部
35
7
17
電源部
12
5

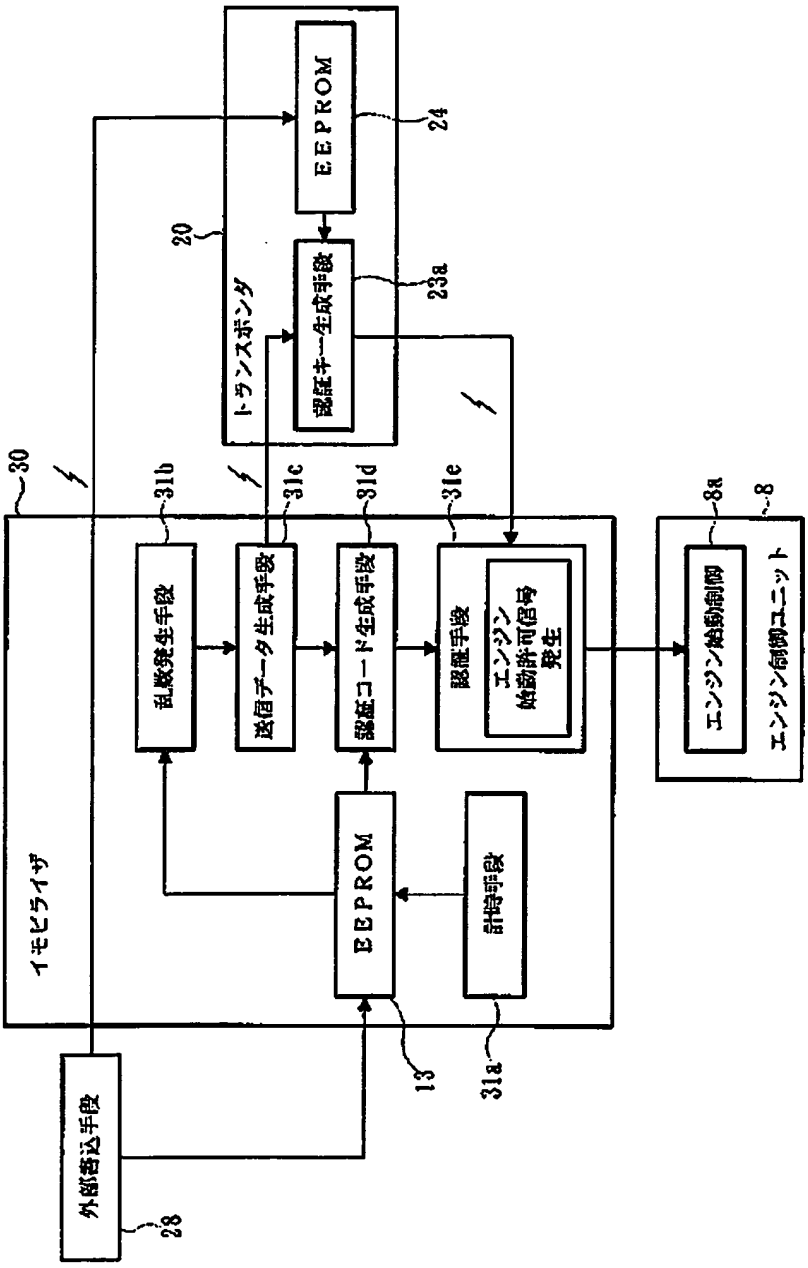
【図3】


EEPROM
24
20
トランスポンダ
認証キー生成手段
23a
10
11b
11c
11d
11e
2a
2
乱数発生手段
送信データ生成手段
認証コード生成手段
認証手段
エンジン始動許可信号発生
エンジン始動制御
エンジン制御ユニット
イモビライザ
EEPROM
計時手段
エンジン始動信号発生
外部書込手段
13
11a
2b
28

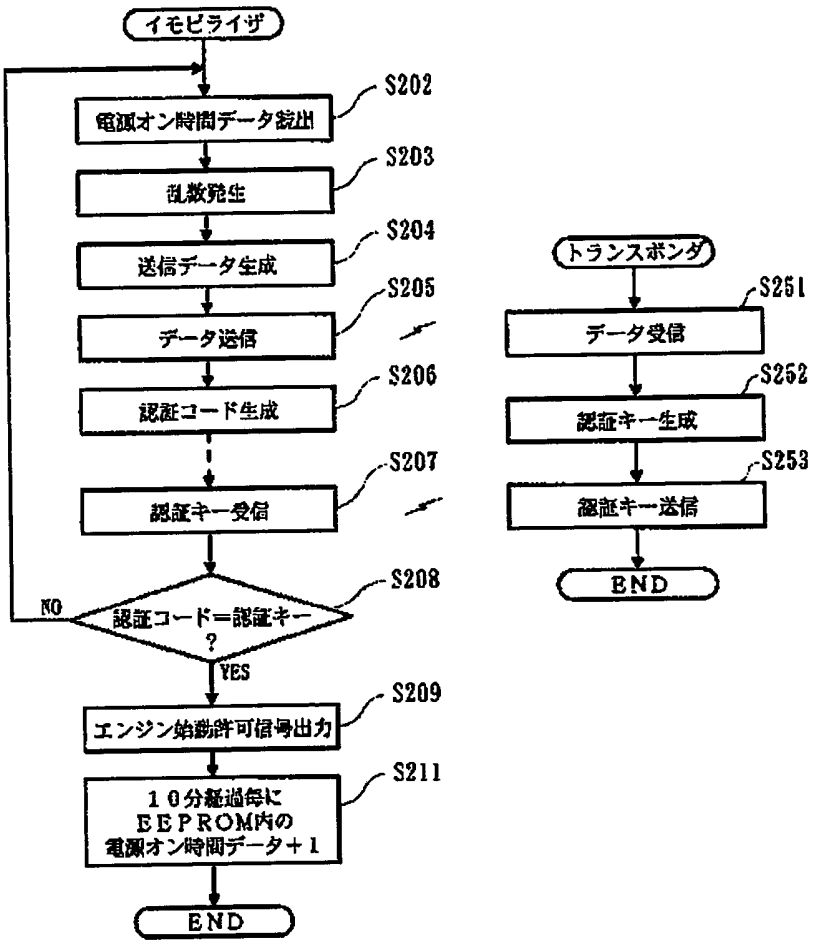
【図4】


イモビライザ
S100
始動時間計時開始
S101
エンジン始動信号
ON
OFF
S102
始動時間データ読出
S103
乱数発生
S104
送信データ生成
S105
データ送信
S106
認証コード生成
S107
認証キー受信
認証コード=認証キー ?
NO
YES
S108
S109
エンジン始動許可信号出力
S111
始動時間計時終了
始動時間データ更新
S112
無線部停止
S113
イモビライザ休止
END
トランスポンダ
S151
データ受信
S152
認証キー生成
S153
認証キー送信
END

【図6】


EEPROM
24
20
トランスポンダ
認証キー生成手段
23a
30
31b
31c
31d
31e
8a
8
乱数発生手段
送信データ生成手段
認証コード生成手段
認証手段
エンジン始動許可信号発生
エンジン始動制御
エンジン制御ユニット
イモビライザ
EEPROM
計時手段
13
31a
外部書込手段
28

【図7】



フロントページの続き

Fターム(参考) 2E250 AA21 BB08 BB66 DD06 EE10
FF26 FF27 FF36 GG05 HH07
JJ05 KK03 LL00 PP15 SS04
TT04
3G084 BA28 CA01 CA07 DA00 EA07
EB06 EC04 FA36
3G093 AA02 BA00 BA26 CA01 DA12
DA13 DB06 EC01 FA11